1-1-1998

Defending Against the Non-State (Criminal) Soldier: Toward a Domestic Response Network

Robert J. Bunker
Claremont Graduate University

Defending Against the Non-State (Criminal) Soldier:

Toward a Domestic Response Network

By Robert J. Bunker, Ph.D., Adjunct Professor, National Security Studies Program, California State University, San Bernardino

Increasingly, national security scholars recognize that the world in which we were born is passing away and, with it, many of the premises, conventions and structures of modern civilization. Research suggests that the transition into the post-modern era will usher in scientific, economic, social, political and military changes of a magnitude never before experienced in American history. Equivalent in scale to the European Renaissance and the Dark Ages, this revolution in political and military affairs, offers both great potentials and dangers for the American public. One of the more fundamental challenges we will face concerns the protection of our citizens. Traditional methods of public policing will become increasingly inadequate as the nature of war changes and assumptions concerning "the rule of law" come into question. Ultimately, the development of a domestic response network will be required if our public institutions are to fulfill the basic security needs of a democratic society.

The Non-State (Criminal) Soldier

One of the more significant attributes of epochal change is the emergence of the non-state (criminal) soldier. Research suggests that this development stems from the failure of the dominant state to remain relevant to the requirements of new forms of civilization, energy sources and developing technologies. As the transition to the post-modern epoch proceeds, the failed-state phenomenon will become an increasingly global issue. Within these former nation-states, war and crime has fully blurred. Conflict has become an intra-state rather than an inter-state activity, with the focus on tribal and ethnic divisions and fragmented social structures based on "haves" and "have nots." The combatants no longer represent the public institutions of the state, but rather non-state entities such as terrorist and guerrilla groups, private armies and security firms, militias, narco-cartels and other criminally based organizations.

Domestically, we must be concerned about the metamorphosis of disenfranchised citizens into non-state soldiers within the United States in the decades to come. In his November 1997 *Crime & Justice International* article, "Third-Generation Street Gangs: Turf, Cartels and Net-Warriors," law enforcement professional and analyst John Sullivan discusses the likely rise of a mercenary-type street gang based on power or financial acquisition goals, with fully evolved political aims. An analysis of linkages between San Diego and Chicago street gangs and the Arellano-Felix cartel in Mexico and the Libyan government, respectively, portray the growing internationalization of some of these criminal groups. If only 1 percent of the estimated 650,000 to 1 million street gang members were to develop into Net-Warriors (a "cyber" form of post-modern soldier), there would be a considerable insurgent force with which to contend within the continental United States.

Segments of other disenfranchised groups within American society must also be considered for their potential to evolve into non-state soldiers. The anti-government Patriot or Militia movement of recent years is also of concern. The Southern Poverty Law Center estimated that 858 active Patriot groups existed in the United States in 1996, and that they were attempting to create a national militia intelligence network. Motorcycle gang members tied into criminal enterprise networks, violent anti-abortionists such as Phineas Priests, malicious hackers allied to various cybertribes, and body armor-clad, assault gun-toting criminals are among the growing list of those who may pose security issues because of their propensity for acts of domestic terrorism.

Nation-State Capability Gap

The public institutions of the nation-state were never designed to counter such an unconventional threat. Law enforcement is meant to contend with a minimal level of crime within a relatively peaceful society. The armed forces address *external* threats to such a society by confronting the armed forces of other nation-states. Non-state forces disrupt the natural order of the international system because of the gray area between crime and war within which they exist. Further, the command and control structures of these groups are becoming increasingly sophisticated. Communications via the Internet provide criminal-soldiers with quicker reaction cycles than traditional, hierarchical police and military forces.

Law enforcement is often outclassed when faced with proto-criminal soldiers who employ secondary devices to kill first responders, religious fanatics who use nerve agents in transit systems, or drug posse members who use hand grenades or assault-type weapons. Similarly, Western military forces have tremendous difficulty operating in failed-state environments against local militiamen who use mobs of women and children as human shields and strike at weak points such as troop barracks with truck bombs.

As a result of this capability gap, police and military functions have a tendency to blur toward each other. Domestically, this can be seen with the rise of Tactical Operations Units (TOUs)— also known as Special Weapons and Tactics (SWAT) teams— which are meant to contend with high-risk situations. In their March 1997 *Police Chief* article, "Tactical Operations Units: A National Study," Dr. Peter Kraska and Larry Gaines reported that 89 percent of non-federal U.S. law enforcement agencies with at least 100 sworn officers and populations of more than 50,000 had TOUs. Used far more frequently than ever

before, these units are regularly armed with tactical headsets (77 percent), night vision equipment (76 percent) and military-style weaponry such as HK MP5s (83 percent) and M-16s (61 percent).

On the flip side, U.S. armed forces that are deployed for stability and support operations in failed states now recognize the value of military-police units, various forms of less-lethal weaponry and public relations with the media. This is because American soldiers are increasingly being held accountable for the well-being of the non-combatant citizens in their area of operations. Rather than assuming the traditional role of occupation forces of a vanquished nation-state, American troops increasingly operate more like a global police against a different enemy—the spread of chaos and anarchy.

Private Security Forces and Mercenaries

Periods of epochal change are also marked by the proliferation of private security forces and mercenaries. Because of both real and perceived vulnerability to lawlessness and criminality, these private armies contract out to individuals, businesses and even governments to provide security services.

Domestically, private security guards far outnumber public police officers, with this trend intensifying. In Dallas, private security guards now outnumber local law enforcement officers by about seven to one. In other areas of the country, such as South Florida, the firm Critical Intervention Services (CIS) is being used to patrol failed communities represented by low-income housing tracts. With their bullet-resistant vests and .357 magnums, these security forces dress to intimidate.

In regions across the country, private gated communities and complexes are mushrooming, as many citizens decide to withdraw from public areas and wall themselves and their families off from the dangers around them. Firms such as Pinkerton's, Inc., and Kroll Associates, Inc., are expanding their influence as top corporate clients seek to better protect their business operations and personnel. Since 1997, Pinkerton's has been offering businesses around-the-clock Suspicious Package Evaluation Teams to quickly scan suspicious parcels on site.

This trend toward the privatization of "public defense" is also evident in foreign stability and support operations where calls for "mercenary peacekeepers" have become increasingly frequent. Besieged underdeveloped countries, the United States and even the United Nations are now involved in varying degrees with the hiring of private security forces and mercenaries for operations in failed or failing states.

Why a Domestic Response Network?

The very real danger is that the public institutions of the nation-state may not be able to respond in a "not war-not crime" operational environment. If our people are unable to live, work and raise their families in relative peace, then the state has failed to provide for the common defense. There is also a real concern that private security firms may begin to usurp the position of public law enforcement agencies in protecting our people. Basic protection would then become a commodity sold to the highest bidder, rather than a public good guaranteed by the constitution.

This strategic-level domestic security dilemma has not yet been fully recognized by the government, which has been focused on the more immediate danger of the non-state soldier threat—the eventual employment of weapons of mass destruction (WMDs) by international or domestic terrorists. While a centralized federal approach is fine for dealing with conven-

tional threats to national security, it is less effective in addressing the new threats developing from the post-modern security environment.

Ultimately, what will be required in support of federal directed efforts is a state, county, and municipal level public, and probably private, integrated network to emerge in support of the qualitatively different domestic security requirements of the 21st century. Rather than a centralized approach to crisis and consequence management, this would be a "webbed" structure based upon a nodal organizational scheme.

Such "semi-leaderless and leaderless networks" can provide many benefits in support of traditional public law enforcement agencies and other first responders. First, they increase the information flow among agencies as data and knowledge are shared outside of traditional hierarchies and bureaucratic fiefdoms. This helps to eliminate informational seams—a key vulnerability within the emerging "cyber" battlespace.

Second, these networks allow a joint approach to identifying and solving (or neutralizing) problems. Trends, incidents and events are analyzed in parallel to each other simultaneously across the network. A physical, phone or virtual query can be analyzed by the rest of the network. Over time, this allows the network to develop a shared image of the state it is attempting to achieve.

Third, networks possess reaction cycles far superior to those of hierarchical structures. In an ever-changing environment, such as during a WMD incident, the crisis management team's ability to be proactive, rather than reactive, is critical.

Fourth, virtual reachback and support capabilities emerge where none existed before. A TOU member with a computer link and direct camera-feed to HAZMAT or bomb disposal personnel has a significant advantage in making immediate life-and-death decisions.

Early Domestic Response Networks

The benefits of a networked approach to countering street gangs, domestic terrorism, drug trafficking and other emergent domestic security concerns have increasingly been recognized by a dynamic group of entrepreneurial law enforcement, emergency responder, military and national security professionals. Three of these networks are institutionally sanctioned; the fourth is a private, free-standing, open-source intelligence group. All can be considered both "informational bridges" between traditional hierarchical agencies and new proto-entities themselves. Because most of these networks are experimental in nature, they tend to represent a trial-and-error process of inter-agency and even inter-sector (government, academia and industry) cooperation. Being so new, they are also typically underfunded, and rely heavily on participants' donations of additional time, effort and funds to keep them viable in their early stages of development.

Early networks appear to be of two types. The first is physically based, bringing together professionals from across agency jurisdictions to meet each month in a centralized location. In crisis situations, the network can be activated by means of pagers or fax lines. The second type is virtual-based, operating as a closed, unclassified information-sharing group using either an electronic mailing list and/or a secure Web site location. Hybrid networks are dual-dimensional in nature, combining both physical and virtual characteristics.

Most of these networks seem to be emerging first in the extended Los Angeles and San Diego metropolitan regions, which were early centers of street gang

and cross-border drug cartel activity respectively.

In Los Angeles, county sheriff's department members have used this network approach first to combat street gangs and now to address domestic terrorism. The Southern California Gang Investigators' Association, originally established in 1977, has not only spread throughout California but replicated itself in network associations across the United States. This mature network of primarily law enforcement, probation, parole and prosecution agencies has been tracking gang members via the Gang Reporting, Evaluation and Tracking (GREAT) system since the mid- to late 1980s. Today, a second-generation system known as CAL/ GANG, which is a Web-based application, is further extending this network by allowing for better cross-departmental cooperation.

Inaugurated in April 1996, the Los Angeles County Terrorism Early Warning Group (TEW), based at the County Emergency Operations Center, has emerged as an integral component of the Los Angeles Operational Terrorism Response & Management Plan, providing the link between existing crisis and threat warning capabilities and the local emergency response community. This experimental physical network is even more comprehensive than the more mature one directed toward street gangs. Its membership and linkages include city, county and federal law enforcement and emergency services, infrastructure and support, national laboratories, private industry, the military and academia both within and outside of Los Angeles County. As this network begins to generate national interest, similar networks are being established in such major urban centers as San Francisco, San Diego and Las Vegas.

Closer to San Diego, there are the physically based Imperial Valley Drug Coalition (IVDC) in Imperial County and Get-The-Word-Out Intelligence (G2i), which is headquartered in San Diego, but operates exclusively on the Internet.

Conceptually linked to the TEW, the IVDC is deliberately organized much like the drug trafficking organizations against which it is directed. According to its coordinator, its strengths include "unobstructed communication across traditional bureaucratic lines, redundant information paths and rapid mini-task force implementation to exploit short-term tactical situations." The mission of this network is to coordinate the assets of 21 participating law enforcement and governmental agencies in support of the U.S. Attorney, San Diego Specialized Drug Enforcement Operations. These counter-drug operations focus on deterring, detecting and interdicting the flow of illegal drugs in and around Imperial County. As the coordi-

nating element for the IVDC, the Law Enforcement Coordination Center facilitates the planning, coordination, operations and intelligence process.

Formed in September 1996, G2i provides assistance to Defense Department intelligence and counterintelligence personnel by providing open-source intelligence (OSINT) useful to their missions. Selected members of civilian law enforcement, private OSINT professionals and academics with specialized, national security-related expertise are also allowed membership in this listserver. Members can be found globally, depending on duty stations and force deployments, but the majority tend to be spread throughout the continental United States.

G2i generates many e-mail messages based on posting guidelines daily, along with numerous queries about specific in-

The L.A. County TEW: A Cooperative Intelligence and Warning Framework for Combating Terrorism

The mission of the Terrorism Early Warning (TEW) group is to monitor trends that could result in terrorist threats or attacks in Los Angeles (L.A.) County. The group evaluates open-source intelligence (OSINT) and research information about threats in order to guide the training and planning efforts of the interagency Terrorism Working Group (TWG). These early warning efforts also support fire service and other emergency response efforts. The TEW works to identify precursor events, with an eye toward prevention and mitigation.

Monitoring Trends and Potentials

Since its inaugural meeting in April 1996, the TEW has been a vehicle for analysis of the strategic and operational information needed to combat terrorism and protect critical infrastructure. Special emphasis is placed on early detection of emerging threats, including weapons of mass destruction, such as nuclear, biological or chemical (NBC) agents, and information warfare (or cyber-terrorism). The TEW supports the County Emergency Operations Center, the interagency TWG and the L.A. County Metropolitan Medical Strike Team. The TEW is coordinated by the Sheriff's Emergency Operations Bureau, which serves as the group's permanent secretariat.

The TEW will join with criminal intelligence groups (such as the L.A. Task Force on Terrorism) to provide the "unified command" at a terrorist incident with a net assessment of response capabilities and the projected "event horizon." To develop the skills necessary to assess trends and potentials and conduct a net assessment, the TEW group conducts regular briefings on such topics as

- chemical and biological terrorism
- advanced terrorism concepts and the non-state soldier
- future war and terrorism (terrorism in a strategic context)
- cross-border potentials
- recent trends (gangs, mercenaries and drugs)
- chlorine attacks and railway bombings in New South Wales
- critical infrastructure protection—telecom
- water system vulnerability
- airbase defense for civil aviation
- counter-terrorism technology issues
- OSINT analysis
- electromagnetic (EM) terrorism potentials
- advanced less-lethal weaponry
- improvised EMP devices
- RF weapons
- Chemical, Biological Incident Response Force (CBIRF) operations and medical capabilities
- the Henderson, NV, "anthrax" incident
- Skinheads and White Supremacists
- Phineas Priests
- problem-solving with biological agents
- nuclear detection issues
- anti- and counter-terrorist technology, including medical technology for mitigating NBC agents and technology for countering cyber-terrorism

Presenters, Participants and Guests

The guest presenters and lecturers at the briefings—all of them experts in their fields—include members of TEW, practitioners and distinguished scientists and policy analysts from throughout the United States. The following agencies and organizations have all been represented: the Emergency Response Research Institute, the FBI, G2i, GTE, the Imperial Valley Law Enforcement Coordination Center, the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, the L.A. County Department of Health Services-EMS Agency and Disease Control Programs, the L.A. police and sheriff's departments, the Metropolitan Water District, the National Security Studies Program at California State University-San Bernardino, the RAND Corporation, Sandia National Laboratories, Scientific Applications Research Associates (SARA Labs), The Simon Weisentahl Center and the U.S. Marine Corps' CBIRF.

Participating agencies are classified as either core or cooperating. The core agencies are the L.A. police and sheriff's departments, the city fire department, the county fire and health services departments, and the L.A. division of the FBI.

The cooperating agencies include the California Office of Emergency Services-Law Enforcement Branch; Federal Aviation Administration Security; the Long Beach police, fire and health departments; Long Beach Emergency Management; the L.A. Department of Airports; the L.A. County District Attorney's Office; the Metropolitan Transportation Authority; the National Security Studies Program at California State University-San Bernardino; the RAND Corp.; and U.S. Customs.

Guests at TEW briefings have included representatives from ATF's L.A. field office, the California Department of Justice, the California National Guard, the California Office of Emergency Services-Fire Branch, the San Francisco and San Diego field offices of the FBI, G2i, GTE/BBN, the Imperial Valley Law Enforcement Coordination Center, the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, the National Law Enforcement and Corrections Technology Center-Western Region, Sandia National Laboratories, SARA Labs, the San Bernardino and San Diego sheriff's departments, and the U.S. Marine Corps.

TEW Reports

In addition to monthly OSINT reports, the TEW has produced the following information papers: "Domestic Terrorism: Army of God," "Domestic Terrorism: Phineas Priests" and "A Bio-Conspirator? Larry Wayne Harris: An Open-Source Profile" (public safety-sensitive). Created for the internal use of the TEW, these documents are designed to educate participants about current issues and build participants' analytical skills. ❖

telligence and point-of-contact membership needs.

While all four of these networks have come in contact with each other, the three newer networks have developed more open-channel linkages and, as a result, may have begun to generate a limited synergy. This can be better understood by examining a ground-breaking incident that took place in January 1998.

The Ricin Alert Incident

On January 6, 1998, a San Diego television station aired a news report concerning a "rumor" that drug traffickers were using a chemical warfare agent to booby-trap loads of methamphetamine. Reportedly, this substance would produce a toxic gas, with effects similar to Mustard Gas, that would be harmful or fatal to law enforcement or military personnel conducting a presumptive drug test. This report apparently originated with an Officer Safety Bulletin from a San Diego law enforcement agency, whose origins can be traced back to a narcotics group bulletin from Kansas.

The news report was seen by a law enforcement officer, who related it during a briefing attended by members of a drug interdiction team on January 7. One of those officers sent a private e-mail message to the G2i moderator, who forwarded it immediately to the chief analyst of the virtual-based Emergency Net News Service (ENN) headquartered at the private Emergency Response & Research Institute in Chicago. On January 8, a request for information was posted on the G2i network on behalf of this law enforcement officer, while ENN simultaneously conducted its own investigation. Early research conducted by a G2i member seemed to rule out Mustard Gas, but because this was only a general perception, further verification was requested. Shortly after that posting, an emergency management professional in Texas tracked down a U.S. Border Patrol Intelligence Safety Bulletin that identified the CW-type agent as Ricin, a deadly toxin. That bulletin is believed to have been derived from the same bulletin that was generated by the narcotics group in Kansas.

Because of the potentially deadly implications of these postings, they immediately generated intense G2i activity in the general listserver, as well as in private e-mails, faxes and phone conversations not only within G2i but also involving agencies and groups with nodes in this virtual network. Queries were made into the validity of the safety bulletin and the inconsistency concerning the production of Mustard Gas as a byproduct of analyzing suspected narcotics with a field testing kit.

Segments of L.A.'s TEW group and the IVDC networks quickly obtained conflicting reports concerning the accuracy of the bulletin in question. By comparing their information and sources, they were able to jointly confirm that the bulletin was invalid—no known or suspected use of Ricin by drug traffickers had taken place. Within six hours of the original G2i posting, a member associated with one of these networks posted a non-law enforcement attribution message stating that the original safety bulletin was inaccurate and that no chemical or biological warfare agent was involved. Those individuals with a vital need to know were placed in contact with the law enforcement personnel and/or agencies who had verified that the alert was inaccurate. Over the course of the next day, concerns over the bulletin subsided as more information came in on the general listserver and G2i members with technical expertise verified that it was chemically impossible for Ricin to produce Mustard Gas.

We must ask ourselves—while we still have the time to prepare—whether we are going to place our trust in private security forces and gated communities, or take the responsibility for ensuring that our public law enforcement institutions will be up to the challenges of the future.

The incident entered its second phase on January 13, 1998, when a new posting on G2i concerning a Ricin alert came in from a public safety professional in New York. It turned out that the original safety bulletin had been widely disseminated and then rebroadcast by a major California agency as another variation of the original alert. Because of the non-linear nature of this incident, ENN was also sent an e-mail that same day from another California agency about this new bulletin. Luckily, the East Coast professional who posted his message on G2i had remembered the earlier discussion on this topic and simply sought confirmation of its inaccuracy. Within a couple of hours, two postings from members of the Los Angeles County TEW network stated that the alert was erroneous. The next day, ENN agreed that the alert was inaccurate and began widespread distribution to subscriber police, fire and emergency medical services agencies in order to help spread the word that the new bulletin concerning this incident was false.

As late as January 16, 1998, reports were still coming into G2i determining that the Ricin alert was bogus, but by then the issue was considered dead and the dreaded Ricin scare was over. Nonetheless, over the course of the next three months, ENN and various law enforcement groups were queried about some sort of Ricin alert. The incident had now become something of an "urban legend," with its suspected origins traced back to a November 17, 1996, *U.S. News & World Report* article on chemical warfare.

The analysis phase of this incident, which occurred from approximately the 14th to the 22nd of January, produced numerous e-mail messages about lessons learned and resulted in a week-long "virtual capture session" concerning what had taken place. Eric Nelson, the G2i moderator, notes the following aspects of the "non-linear, non-hierarchical" joint operation:

- no inter-agency territorialism
- instant linkage of remotely located parties
- constant sharing of information
- joint effort
- rankless and non-linear medium

What can be learned and applied from the Ricin experience on G2i? Nelson observes:

> *It is no small event we have just witnessed. When in the history of the United States has this great a collection of military organizations, civilian law enforcement and academics jointly worked on an important issue from remote locations until it was resolved?*
>
> *This is no mere information distribution network. We are a laboratory that is experimenting with the future: joint operations between military and civilian forces. We are also experimenting with non-linear interconnectivity and non-hierarchical joint efforts.*
>
> *This entire phenomenon bears great thought. It has worked so well that we were days ahead of non-connected agencies, many of whom are still passing bad information.*
>
> *Let's tear this thing apart and figure out how we can do it again.*

Some of these lessons, as well as other Ricin-related news items obtained from information sources outside of G2i, were summarized in an ENN synopsis of the event published on January 18 primarily for general law enforcement and first responder audiences not included in the G2i listserver membership.

It should be noted that just three days prior to that final ENN synopsis, the San Diego Union-Tribune was still reporting that an officer safety alert concerning a toxic poison known as Ricin was being broadcast across the county by a major counter-drug agency and was in turn being picked up by local law enforcement agencies. Fortunately, those progressive law enforcement and governmental organizations that were "webbed" into the experimental domestic response network were already aware that the alert was erroneous.

Conclusions

In order to respond to the challenges facing law enforcement as a result of the rise of the non-state soldier, a domestic response network will be a needed addition to the traditional top-down federal approach to domestic defense. Such a network would represent a natural evolutionary step for the more than 17,000 independent public law enforcement entities found throughout the United States, and would greatly support the federal government in its endeavors to provide for the common defense. Ultimately, such a network would allow those agencies and allied organizations the ability to share information and decrease response times for crisis and consequence management.

As one member of the L.A. County Sheriff's Department notes with respect to the Ricin incident:

> *I think we have demonstrated the value of intelligence support to both crisis and consequence management of emerging threats.... [A]n expanded recognition of the utility of virtual OSINT networks by decision- and policy-makers (not to mention field commanders) is essential to future success.*

Policy makers must begin to fuse open-source information about street and motorcycle gangs, terrorist groups, militias, extremist and hate groups, drug cartel activities (both along the border and internally) and private security forces to obtain a baseline strategic picture of our current domestic security environment. These areas of concern are not unrelated and discrete trends; linked together, they can provide us with important insights into the health of our society.

We must ask ourselves—while we still have the time to prepare—whether we are going to place our trust in private security forces and gated communities, or take the responsibility for ensuring that our public law enforcement institutions will be up to the challenges of the future. If it is to be the latter—as indeed it must be if we are to preserve our constitutional rights and liberties—then a domestic response network will be essential. ❖